NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2011/030911-9-security-tips-for-protecting.html

9 Security Tips for Protecting Mobile Workers

Hugh Thompson offers a set of defenses for keeping data safe, even when it's on the move

By Dr. Hugh Thompson, CSO
March 09, 2011 03:19 PM ET

The new working professional is always connected, and increasingly, the office is Starbucks, an airport, or home. With new flexibility comes new IT security risks for businesses. Basic defenses like antivirus are important, but not enough to keep corporate data from the increasingly sophisticated hacker.

How can mobile workers better protect information while they're outside the office? Here are 9 tips to keep employees (and corporate data) safe outside the office:

Tip 1: Use laptop disk encryption

One of the first lines of defense is to secure data that sits on a laptop's hard drive to make it unpalatably difficult for attackers to retrieve data from a device that slips out of an employee's control. As more personal laptops have entered the work ecosystem, disk encryption has become increasingly important. Without properly implemented encryption, a password is just a polite request for an attacker to not access data.

Tip 2: For laptops, set boot order and password in the bios

Most people have their Windows accounts locked down, but what about the BIOS? The first thing a seasoned attacker will try to do is boot from something other than the hard disk (USB stick, CD, etc.) and poke around. There are a few techniques to make this more difficult. One is to put the hard disk first on the boot list in the BIOS and then password protect the BIOS to stop someone from changing it. If an attacker has stolen the laptop, they can still take more drastic measures such as removing the hard disk (but hopefully it's encrypted --see Tip 1 above). Changing the boot order will make it more difficult for an attacker that has brief access to the machine.

Tip 3: See what it takes to do password resets, then educate employees

The model of using biographical information for password reset is failing. The name of an employee's favorite

pet, grandfather's occupation and mother's maiden name are more available than ever before: attackers can mine information from social networking sites as well as public records that are now online. It's an important exercise for employees to see how exposed they are by trying password resets on their corporate and personal accounts. Imagine they have forgotten all passwords to email, their laptop, etc. How do they reset them? What questions get asked? Could someone find those answers online somewhere? If so, it's time to change those questions or answers. If the account simply sends a password reset email then ask: what would it take for someone to reset an email password?

Tip 4: Educate employees on the risks of public Wi-Fi networks

Free tools abound to sniff traffic on public Wi-Fi networks. With that in mind, it's important for employees to take precautions when accessing or sending anything sensitive (email, searches, etc.). Mobile workers should always ensure that email is sent and received through an encrypted channel (VPN, webmail over SSL, etc.). For corporate email, this should be the only route possible to receive messages. The reality though is that sometimes policies are circumvented in the name of productivity. One common example is sending corporate documents to personal email accounts so that they are easier to access and work with outside the office. If you accept that work-related activities will be done while not connected through a VPN or on a corporate-sanctioned device, it is important to educate employees about the risks and help them make safer choices.

Tip 5: Enable automatic patching

You've turned on automatic update for Windows and Office, but what about the rest of the software on the system? Attackers are diversifying their strategies for machine infection and it's important to keep up to date with patches on all software. In the past, the risk of automatically applying a bad patch --one that caused the system to malfunction --outweighed the risk of leaving the system unprotected till the patch could be thoroughly tested. For mobile workers, that tradeoff needs to be reevaluated for key applications.

Tip 6: Protect visual privacy

Eventually, sensitive data will likely be displayed on a laptop screen, but are mobile workers taking steps to protect it? With the rise in quality of smart phone cameras, it is now possible for data thieves or competitors to take readable pictures of on-screen data at a distance, which increases the importance of protecting visual privacy. Angling screens away from public view or using computer screen privacy filters can help reduce the risk-- but ultimately working professionals need to be mindful of their environment when accessing information that might be of value to someone else. This is particularly important at conferences or seminars where people in the same industry are likely to be in close proximity.

Tip 7: Beware of social networking information leakage

It's easy to reveal too much information while on the road. The most common mistake employees make is to reveal geo-location information. Mentioning that you're in Bentonville, Arkansas for a meeting might not seem like a big deal but a competitor could easily infer that your company has a budding relationship with Wal-Mart, one of the very few companies headquartered there. This type of data might be revealed directly--in a status update on Facebook or Twitter --or it may be revealed indirectly based on the tool used to update Facebook, Twitter or LinkedIn.

Also see The final 5 tweets of Harold Wigginbottom, tech-savvy CEO

Beyond location, employees need to be aware that changes in business relationships on LinkedIn may reveal something interesting (and very confidential) about the business. If someone in the Mergers and Acquisitions Department suddenly adds five people as contacts from a smaller company through LinkedIn it could indicate a relationship.

Finally, employees also need to be aware that anything they post publically might be used against them to add credibility to a phishing email. The growing personalization of email attacks makes it harder to differentiate a real

email from a fake. Employees need to be educated about the risks and be exceptionally cautious with emails that ask them to send sensitive information to addresses outside the company.

Tip 8: Set up remote wipe for mobile devices

What happens when an employee reports a mobile device is missing? In most cases, data contained in the device is much more important (and valuable) than the device itself, especially when it comes to corporate information. Most smart phones support remote wipe. By setting up remote wipe on corporate-issued devices (and if possible, on employee-owned devices that are allowed to access corporate email) you're taking insurance against theft or loss of the device. If attackers have unfettered access to the device, however, they may be able to download the data first and even disable remote wipe. This ties into Tip 9.

Tip 9: Lock mobile devices

In the battle of convenience vs. security, convenience often wins. When employees use a mobile device to access corporate data it's important to educate them about the importance of locking their devices. Locking the device is a delay mechanism if the device is lost or stolen. It buys you time to either remotely wipe the device when it is reported missing or do something more elaborate like find it via GPS. Many devices can also be set to wipe themselves after a set number of incorrect login attempts. Even if a device is setup for remote wipe, leaving it unlocked can sometimes allow thieves to disable those settings before you've had a chance to issue a wipe command.

Ultimately, protecting corporate and personal data requires that employees be on guard. Applying these tips will help avoid some of the biggest threats on the road.

Dr. Herbert Hugh Thompson is Chief Security Strategist at People Security and a consultant for 3M Privacy Filters. He is also an adjunct professor at Columbia University.